

### **EXAMINER'S AMENDMENT**

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Greg Johnson (Reg. No. 59,027) on 12/08/2008.

The application has been amended as follows:

#### **IN THE CLAIMS**

1-20. (Canceled)

21. In a sending domain that is network connectable to one or more receiving domains, the sending domain including a sending messaging server configured to send electronic messages to the receiving domains, a method for indicating to a receiving side domain that the sending messaging server expended computational resources to solve a predetermined computational puzzle before sending an electronic message to the receiving side domain, the method comprising:

an act of the sending messaging server receiving electronic message data that is to be contained in an electronic message sent from the sending messaging server to the receiving side domain;

an act of the sending messaging server generating puzzle input from one or more components of the electronic message, the one or more components selected from a group consisting of: a message body, a message attachment, and a message header, and wherein the act of generating puzzle input includes one or more of: extracting portions of at least one of the one or more components, hashing portions of at least one of the one or more components, and concatenating portions of at least one of the one or more components;

an act of the sending messaging server identifying an answer document by applying a hashing algorithm to different answer documents until the hashing algorithm produces an answer hash value that is a solution to the predetermined computational puzzle,

wherein the answer hash value is calculated by:

combining one of the different answer documents and the puzzle input; and

hashing the combination of the one of the different answer documents and the puzzle input using the hashing algorithm, wherein the hashing algorithm alters a standard application of SHA-1 sub functions; and

an act of the sending messaging server identifying an answer document using the computational puzzle, wherein the act of identifying the answer document further comprises, calculating an answer hash value using a hashing algorithm that alters a standard application of SHA-1 sub functions; and

an act of sending the electronic message from the sending messaging server to the receiving side domain, wherein the electronic message includes the identified answer document and the electronic message data enabling verification by the receiving side domain that the sending messaging server expended computational resources without further communication with the sending messaging server.

22. The method as recited in claim 21, wherein the act of the sending messaging server receiving electronic message data that is to be contained in an electronic message comprises an act of receiving electronic message data that is to be contained in an electronic mail message.

23. The method as recited in claim 21, further comprising an act of generating an initial document from at least one of the one or more components, wherein the act of generating the initial document comprises extracting data from at least one field of the electronic message data wherein the at least one field is selected from a From field, a

To field, a NotBefore field, a NotAfter field, a Date field, a Body field, an Attachment field, a Subject field, and a Message-Id field.

24. The method as recited in claim 23, wherein the act of generating an initial document from at least one of the one or more components comprises an act of extracting data from one or more date range fields.

25. The method as recited in claim 23, wherein the act of generating an initial document from at least one of the one or more components comprises an act of extracting data wherein the data is text data, graphical data, Uniform Resource Identifier ("URI") data, or executable data.

26. The method as recited in claim 21, wherein the act of the sending messaging server identifying an answer document comprises an act of identifying an answer document that, when combined with the puzzle input and the combination of the answer document and puzzle input is hashed, results in a hash value having a specified value in a plurality of fixed bit positions.

27. The method as recited in claim 26, wherein the act of the sending messaging server identifying an answer document comprises an act of identifying an answer document that, when ~~prepended~~ prepended to the puzzle input and the concatenation of the answer document and puzzle input is hashed, results in a hash value having a value of zero in at least a first specified number of bits.

28. The method as recited in claim 21, wherein the act of the sending messaging server identifying an answer document comprises an act of identifying an answer document that, when concatenated to the puzzle input and the concatenation of the answer document and puzzle input is hashed, results in a hash value having specified bit values in a first plurality of bit positions and having bit values equal to the corresponding bit values of the hashes resulting from other answer documents in a second plurality of bit

positions.

29. The method as recited in claim 28, wherein the act of the sending messaging server identifying an answer document comprises an act of identifying an answer document that, when concatenated to the puzzle input and the concatenation of the answer document and puzzle input is hashed, results in a hash value having specified values in each bit position of a hash value prefix and a value equal to corresponding hash bit values resulting from other answer documents in a hash value suffix.

30. The method as recited in claim 21, wherein the act of the sending messaging server identifying an answer document comprises an act of using [[an]]a puzzle hash algorithm, the puzzle hash algorithm being specifically designed to increase the difficulty of implementing hardware acceleration of the puzzle hash algorithm.

31. (Canceled)

32. The method as recited in claim 21, wherein the act of sending an electronic message that includes the identified answer document and the electronic message data to the receiving side domain comprises an act of sending an electronic message that includes a plurality of answer documents.

33. The method as recited in claim 21, further comprising: an act of querying a server to determine if the receiving domain is configured to verify answers to computational puzzles; and an act of receiving one or more DNS TXT records that contain electronic message configuration information for the receiving domain.

34. The method as recited in claim 33, wherein the act of querying a server comprises an act of querying a server in response to the sending domain not supporting electronic mail transmission policy certificates.

35. The method as recited in claim 33, wherein the act of receiving one or more DNS TXT records comprises an act of receiving one or more DNS TXT records that encode the electronic message configuration information in XML instructions

36. In a receiving domain that is network connectable to one or more sending domains, the receiving domain including one or more receiving messaging servers configured to receive electronic messages from the sending domains, a method for determining if a sending messaging server solved a predetermined computational puzzle before sending an electronic message, the method comprising:

- an act of receiving an electronic message that includes electronic message data and an answer document;

- an act of ~~recalculating~~ reproducing a puzzle input from one or more predetermined components of the electronic message, the one or more predetermined components selected from a group consisting of: a message body, a message attachment, and a message header, [[and]] wherein reproducing puzzle input ~~recalculation~~ includes one or more of: extracting portions of at least one of the one or more predetermined components, hashing portions of at least one of the one or more predetermined components, and concatenating portions of at least one of the one or more predetermined components, and wherein the act of reproducing~~recalculating~~ a puzzle input from one or more predetermined components of the electronic message further comprises an act of applying a hashing algorithm that alters the standard application of SHA-1 sub-functions;

- an act of determining if a verifying hash value, ~~calculated from a combination of the answer document and the puzzle input, is an answer value indicative of a solution is~~ a solution to the predetermined computational puzzle, the verifying hash value being calculated by combining the answer document and the puzzle input and hashing the combination of the answer document and puzzle input using the hashing algorithm; and

- an act of providing results of the determination to a message classification module wherein the message classification module determines, based on the results,

whether the received electronic message is spam.

37. The method as recited in claim 36, wherein the act of receiving an electronic message that includes electronic message data and an answer document comprises an act of receiving an electronic mail message.

38. The method as recited in claim 36, wherein the act of receiving an electronic message that includes electronic message data and an answer document comprises an act of receiving an electronic message that includes a plurality of answer documents.

39. The method as recited in claim 36, further comprising an act of reproducing an initial document from at least one of the one or more predetermined components of the electronic message, wherein the act of reproducing the initial document comprises an act of extracting data from a field of the electronic message data wherein the field is selected from among a From field, a To field, a NotBefore field, a NotAfter field, a Date field, a Body field, an Attachment field, a Subject field, and a Message-ID field.

40. The method as recited in claim 39, wherein the act of reproducing an initial document from at least one of the one or more predetermined components of the electronic message comprises an act of extracting data from the electronic message data wherein the data is text data, graphical data, Uniform Resource Identifier ("URI") data, or executable data.

41. The method as recited in claim 36, wherein the act of ~~recalculating~~ reproducing a puzzle input from one or more predetermined components of the electronic message comprises an act of applying the hashing algorithm, the hashing algorithm being specifically designed to increase the difficulty of implementing hardware acceleration used to enhance efficiency of the hashing algorithm.

42. (Canceled)

43. The method as recited in claim 36, wherein the act of determining if a verifying hash value, calculated from a combination of an answer document and the puzzle input, is an answer value indicative of a solution to the predetermined computational puzzle comprises an act of determining if the verifying hash value has a specified value in a plurality of fixed bit positions interspersed throughout the verifying hash value.

44. The method as recited in claim 36, wherein the act of determining if a verifying hash value, calculated from a combination of an answer document and the puzzle input, is an answer value indicative of a solution to the predetermined computational puzzle comprises an act of determining if the verifying hash value has a specified value in a first plurality of bit positions and has a value equal to other verifying hash values resulting from other answer documents in a second plurality of bit positions.

45. (Canceled)

46. A computer program product for use in a sending domain that is network connectable to one or more receiving domains, the sending domain including a sending messaging server configured to send electronic messages to the receiving domains, the computer program product for implementing a method for indicating to a receiving side domain that the sending messaging server expended computational resources to solve a predetermined computational puzzle before sending an electronic message to the receiving side domain, the computer program product comprising one or more computer storage media having stored thereon computer executable instructions that, when executed by a processor, cause the sending domain to perform the following:

- receive electronic message data that is to be contained in an electronic message;

- generate puzzle input from one or more components of the electronic message, the one or more components selected from a group consisting of: a message body, a message attachment, and a message header, and wherein puzzle input generation

includes one or more of: extracting portions of at least one of the one or more components, hashing portions of at least one of the one or more components, and concatenating portions of at least one of the one or more components;

identify an answer document by applying a hashing algorithm to different answer documents until the hashing algorithm produces an answer hash value that is a solution to the predetermined computational puzzle,

wherein the answer hash value is calculated by:

combining one of the different answer documents and the puzzle input;

and

hashing the combination of the one of the different answer documents and the puzzle input using the hashing algorithm, wherein the hashing algorithm alters a standard application of SHA-1 sub functions; and

identify an answer document using the computational puzzle, wherein identifying the answer document comprises calculating an answer hash value using a hashing algorithm that alters a standard application of SHA-1 sub functions; and

send the electronic message to the receiving side domain, wherein the electronic message includes the identified answer document and the electronic message and enables verification by the receiving side domain that the sending messaging server expended computational resources without further communication with the sending messaging server.

47. A computer program product for use in a receiving domain that is network connectable to one or more sending domains, the receiving domain including one or more receiving messaging servers configured to receive electronic messages from the sending domains, the computer program product for implementing a method for determining if a sending messaging server solved a predetermined computational puzzle before sending an electronic message, the computer program product comprising one or more computer storage media having stored thereon computer executable instructions that, when executed by a processor, cause the receiving domain to perform the following:

receive an electronic message that includes electronic message data and an answer document;

~~recalculate~~ reproduce a puzzle input from one or more predetermined components of the electronic message, the one or more predetermined components selected from a group consisting of: a message body, a message attachment, and a message header, ~~[[and]]~~ wherein reproducing puzzle input ~~recalculation~~ includes one or more of: extracting portions of at least one of the one or more predetermined components, hashing portions of at least one of the one or more predetermined components, and concatenating portions of at least one of the one or more predetermined components, and wherein ~~recalculating~~ reproducing a puzzle input from one or more predetermined components of the electronic message comprises an act of applying a hashing algorithm that alters the standard application of SHA-1 sub-functions;

determine if a verifying hash value, ~~calculated from a combination of the answer document and the puzzle input, is an answer value indicative of a solution~~ is a solution to the predetermined computational puzzle, the verifying hash value being calculated by combining the answer document and the puzzle input and hashing the combination of the answer document and the puzzle input using the hashing algorithm; and

provide results of the determination to a message classification module such that the message classification module determines, based on the results, whether the received electronic message is spam.

48-53. (Canceled)

### ***Reasons for Allowance***

The following is an examiner's statement of reasons for allowance:

Claims 21-30, 32-41, 43-44, and 46-47 are allowed in view of the Applicant's arguments (see Applicant's Response, filed 10/17/2008) and the cited prior art of

record. The independent claims 21 and 46 recite a sending messaging server performing a predetermined computational puzzle to show that the sending messaging server spent computational resources to send an email, the predetermined computational puzzle involving performing a hashing algorithm that requires generating puzzle input from the email, and determining what answer document value, which when combined with the puzzle input and then hashed, will provide a solution to the predetermined computational puzzle which, in addition to the rest of the claim limitations, are distinguished from the prior art. Independent claims 36 and 47 recite a receiving messaging server performing the same hashing function using the answer document value calculated by the sending messaging server to determine that the sending messaging server spent computational resources to send the email, which, in addition to the rest of the claim limitations, are distinguished from the prior art. For support, see Instant Specification (See corresponding publication 2004/0181585, Figure 7 and paragraphs [0105]-[0115]).

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JERRY DENNISON whose telephone number is (571)272-3910. The examiner can normally be reached on M-F 8:30am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tonia Dollinger can be reached on (571) 272-4170. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J. Bret Dennison/  
Examiner, Art Unit 2443